PRIVACY AND THE EMERGING INTERNET OF THINGS: USING THE FRAMEWORK OF CONTEXTUAL INTEGRITY TO INFORM POLICY

Jenifer S. Winter
University of Hawai'i at Mānoa
U.S.A.

ABSTRACT

The Internet of Things is an emerging global infrastructure that employs wireless sensors to collect, store, and exchange data. Increasingly, applications for marketing and advertising have been articulated as a means to enhance the consumer shopping experience, in addition to improving efficiency. However, privacy advocates have challenged the mass aggregation of personally-identifiable information in databases and geotracking, the use of location-based services to identify one's precise location over time. This paper employs the framework of *contextual integrity* related to privacy developed by Nissenbaum (2010) as a tool to understand citizens in Hawaii's response to specific implementations of Internet of Things-related technologies. The purpose of the study was to identify and understand specific changes in information practices that will be brought about by the Internet of Things that may be perceived as privacy violations. Specifically, what changes in actors, attributes, and transmission principle related to the Internet of Things can be identified, and what do these reveal about underlying norms? Eight citizens were interviewed, read a scenario of near-term Internet of Things implementations in the supermarket, and were asked to reflect on changes in the key actors involved, information attributes, principles of transmission. Areas where new practices occur with the Internet of Things were then highlighted as potential problems (privacy violations). Issues identified included the mining of medical data, invasive targeted advertising, and loss of autonomy through marketing profiles or personal affect monitoring. While there were numerous aspects deemed desirable by the participants, some developments appeared to tip the balance between consumer benefit and corporate gain. Their surveillance power creates an imbalance between the consumer and the corporation that may also impact individual autonomy. The policy implications of these findings are discussed.

KEYWORDS

Privacy, Internet of Things, Policy, Framework of Contextual Integrity, Surveillance, RFID, location-based systems (LBS)

1. INTRODUCTION

The Internet of Things is an emerging infrastructure that employs radio frequency identification (RFID), near field communication (NFC), and related technologies to "enable the Internet to reach out into the real world of physical objects" (Internet of Things Conference, 2010). There is not a single definition for the Internet of Things – rather, it describes a variety of developments in which everyday objects can be tagged, and using standards enabling unique identification, communicate over the Internet. Weber and Weber (2010) see the Internet of Things as a "backbone for ubiquitous

computing, enabling smart environments to recognize and identify objects, and retrieve information from the Internet to facilitate their adaptive functionality” (p. 1). Thus, it can be seen as a global architecture permitting enhanced intelligence to facilitate the exchange of goods and services. In addition to networking objects for supply chain management, the ubiquitous integration of tags and sensor networks may also be employed in smart appliances, smart homes, and in-vivo health applications.

Visions of the Internet of Things rely, in part, on the rapid increase in the amount of data collected and exchanged due to an explosion in the number of communication devices, what The European Commission Information Society and Media (2008) refers to as a “data deluge” (p. 6). These data are increasingly being used in the manipulation of personal information, or “dataveillance” (Clarke, 1988), in business intelligence and consumer marketing, and the Internet of Things will potentially magnify this trend. Further, the goals of Internet of Things development include empowering computers “with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers to observe, identify and understand the world—without the limitations of human-entered data” (Ashton, 2009, para. 5). Thus, the potential impacts of automated data gathering and data mining must also be considered.

These developments are being marketed to citizens and governments as a means toward greater efficiency, safety, and convenience, as well as an important enabler for developing new services with user-generated content. In addition to the data deluge, RFID makes it possible to harvest a wide array of new data types, enabling data mining to predict consumer behavior, improve supply chain management, and monitor other aspects of the physical environment. However, a great deal of concern has been generated about privacy issues related to the Internet of Things and related technologies. Opponents highlight issues such as the mass aggregation of personally-identifiable information in databases and geotracking, the use of location-based services to identify one’s precise location over time.

Although the surveillance potential of modern information and communication technologies is widely acknowledged, The Internet of Things poses several unique challenges to privacy. First, because many of its components are small and not necessarily visible, one potentially does not know when and where data is being collected. This complicates regulatory or technical schemes that rely on consumer consent. Second, because billions of everyday objects, or even the human body itself, can be equipped with sensors, there are many new types of data that can be collected. Patterns can be sought in information that was previously not analyzed. Further, machine intelligence may be used to both collect and analyze these data. Third, because it is part of a global Internet-based system, data can potentially be aggregated and linked to other personally-identifiable records. Increasingly, global flows of information make it possible for this personal data to be accessed by a variety of sources. These attributes have led to growing recognition of a need for technical standards and governance to “build trust and confidence in these novel technologies rather than increasing fears of total surveillance scenarios” (The European Commission Information Society and Media, 2008, p.3)

When considering the Internet of Things, it is important to acknowledge that it is an emerging environment that cannot be explicitly examined in situ. However, it is not entirely "in the future". Importantly, Dourish and Bell (2011) point out that infrastructures are messy and in constant flux – "thinking of infrastructure as stable, uniform, seamless, and universally available is clearly problematic" (pp. 28-29). The framework for the Internet of Things already exists and features of it are already employed in limited ways.

1.1 PRIVACY AND LEGAL CONCERNS

While privacy is often acknowledged a human right, there is no consensus about what privacy entails or how it can be adequately addressed in policy and law. Because there will be marked changes in the types of data collected, the amount of data collected, and the analyses used to exploit it, the Internet of Things is certain to be a hotbed of privacy concerns. At national or regional levels, the Internet of Things is becoming integral to information and communication technology (ICT) policy initiatives, and privacy concerns are being addressed in various ways. In 2010, China's Ministry of Industry and Information Technology (MIIT) announced plans to make the Internet of Things a key component of IT policy and intends to strengthen relevant financial and taxation measures ("China working on unified national Internet of Things strategic plan", 2010 July 5); however, there is as of yet no specific legal protection. In contrast, the European Union has long had a comprehensive data protection scheme and, in conjunction with its resolution to support Internet of Things development, recently formally addressed privacy concerns about the Internet of Things, adopting an agreement called the Privacy and Data Protection Impact Assessment Framework for RFID Applications as a means to safeguard citizen privacy (O'Connor, 2011).

In the United States, there is no comprehensive law protecting consumer privacy. At the federal level, the *Electronic Communications Privacy Act* (1986) does not adequately address modern information technologies, data aggregation and exchange, and novel information practices. Instead, United States citizens must rely largely on corporate self-regulation and a number of sector-specific privacy laws (e.g., health records). This has not been successful in allaying concern: In December of 2010, the Federal Trade Commission released a report on proposals for consumer privacy (Federal Trade Commission, 2010), and growing concern about abuse of consumer records has recently led to proposals in Congress to reform the 1986 *Act*.

Weber and Weber (2010) note the legal challenges surrounding privacy and Internet of Things development. A first question is whether there is a need for laws to govern these changes or if business self-regulation will suffice. Then, if legislation is the chosen path, are existing laws sufficient? Finally, if new laws are needed, "what kind of laws are required and what is the time frame for their implementation?" (p. 52).

It is important to consider that blanket approaches that rely on a dichotomy between "public" and "private" data may fail to account for certain instances where citizens feel their privacy expectations have been violated. This paper addresses how we can better foster the development of new systems, practices, and policies that support citizens' rights to privacy. Following Kling (2000) and Nissenbaum (2010), it is argued that new technologies such as the Internet of Things are not necessarily positive or negative but

must be viewed in specific context. The framework of contextual integrity related to privacy developed by Nissenbaum (2010) is employed as a tool to understand citizens in Hawaii’s concerns about Internet of Things-related technologies. Specifically, the purpose of the study is to identify and understand specific changes in information practices that will be brought about by the Internet of Things and may be perceived as privacy violations by citizens and to reflect on the underlying norms that shape their perceptions.

1.2 THE FRAMEWORK OF CONTEXTUAL INTEGRITY

Nissenbaum (2010) describes the right to privacy not as a right to secrecy or control, but to “appropriate flow of personal information” or contextual integrity (p. 127). Addressing Facebook executive Mark Zuckerberg’s claim that privacy is no longer a social norm (Barnett, 11 Jan 2010), she proposes the framework in order to guide assessment of new practices arising from technical systems. The question becomes, do novel practices “violate context-relative informational norms?” (p. 148). To address this, a comparison must be made between the existing practice and the new practice. In particular, changes in key actors, types of data collected, and principles of transmission, are explored. Finally, “if the new practice generates changes in actors, attributes, or transmission principles, the practice is flagged as violating entrenched informational norms and constitutes a prima facie violation of contextual integrity.” (p. 150). Once this has been ascertained, ethical factors affected by the new practice are considered in light of the specific context. Thus, the framework of contextual integrity is useful in understanding people’s reactions to information technologies reshaping personal information flows and can be helpful in explaining resistance and fear in response to these changes. This information can then be used to inform system design and policy.

2. METHODOLOGY

This study seeks to identify normative conflicts related to the consumer in-store supermarket experience in the context of the Internet of Things. The supermarket is chosen for analysis because it is a site for a constellation of everyday tasks that are not typically associated with a great deal of privacy concern. Furthermore, information exchanges in this context are not, at present, explicitly protected by federal privacy laws. To explore citizens’ perception about context-specific norms of privacy related to the in-store shopping experience, in-person, semi-structured interviews were administered. Interviews were employed so that the same sets of questions could be used in each interview, while allowing the flexibility to follow important paths.

Participants were elicited based on their status as citizens of the State of Hawaii, having visited a supermarket during the past month, and being users of location-based services on a mobile device. As the Internet of Things is an emerging infrastructure and present location-based services are seen as an important component of it, some familiarity with the types of services discussed was seen as advantageous. In addition, participants were selected to reflect a variety of perspectives based on age, ethnicity, gender and occupation. Recruitment was performed online and on a volunteer basis.

The development of interview questions and analysis was guided by the analytic framework of contextual integrity (Nissenbaum, 2010). Participants were first asked to anchor their responses to a recent supermarket visit. Interview questions then sought to gain insight into their perception of *information attributes*, what types of data they thought might have been collected about them during this visit. This included when they arrived, if they were there with any other individuals, what they looked at or touched, and what they bought. A second set of questions asked participants about the *actors* involved, who they thought had observed these behaviors (human or electronic), and who had access to it or handled this information. Other questions addressed *principles of transmission*, whether data was recorded and how it was transmitted. Once the existing practices and expectations were discussed, the participants read a short scenario describing a visit to the supermarket in the year 2021. The scenario was drawn from a variety of global Internet of Things developments, including present research initiatives and corporate visions, and described the participant visiting the same store that they answered questions about in the first part. After they completed the scenario, a final set of questions addressed changes to the existing practices (and expectations) of privacy. Areas where new practices occurred with the Internet of Things were then highlighted as potential privacy violations and these areas were discussed to probe for underlying norms.

Interviews were recorded with a digital audio recorder, transcribed, and in some cases, clarifying questions were asked of participants to review for accuracy, strengthening objectivity and credibility. Qualitative analysis of the complete transcripts was used to develop themes as they emerged. Transcripts were analyzed and inductively coded using ATLAS.ti Scientific Software. After coding was finalized, data were summarized thematically.

3. RESULTS AND DISCUSSION

A total of eight participants representing both genders, and a variety of age groups, occupations, and ethnicities were interviewed. All participants resided on the island of Oahu and were therefore residents of the City & County of Honolulu. *Table 1* provides a summary of participants. (Pseudonyms are used to protect their identities).

3.1 EXISTING PRACTICES/EXPECTATIONS

Participants uniformly described their visit to the supermarket as a routine shopping experience where they examined and purchased a variety of items. However, interviewees were varied in their expectations of current information practices. The majority suggested that they felt only store employees or other customers might be aware of their arrival or movement throughout the store. However, three participants recalled surveillance cameras. Maile suggested that “If they really wanted to they could go back and check the camera footage.” Kepano and Kainoa indicated that they were aware of constant video surveillance from the moment they entered the store, as theft deterrent or to investigate security issues, as well as for possible review for marketing strategies. Kepano observed, “I’m sure they keep those videotapes around for a while, and I’m sure they’re using it for more than just saving my face in case I rob the place.” Kainoa explained that he had previously worked in a supermarket and that he believes

that surveillance footage may be combed for marketing purposes related to consumer behavior. Participants acknowledged that affiliates, such as manufacturers, might have access to limited data. However, it was emphasized that this should not be linked to specific individuals. There was the expectation that, even though they were in a public place where they might encounter people they knew, their purchases were relatively private.

All interviewees noted owning a rewards card, and in all but one case, such a card was used during the visit in question. There was consensus that information about the items they bought was likely stored in some type of electronic database and would be linked to their identity. There was consensus that use of the rewards card represented an agreement to share limited personal information in exchange for lower prices, special offers and coupons, and more customized suggestions. All believed that the present intent of this gathering was to create a customized experience for the user and to make business operations more efficient in a way that benefitted the consumer – “an acceptable balance”, as Nalani described it. Maka, Anuhea, and Kepano mentioned that it would be inappropriate for any of the information gathered about their activities in the store to be used outside the corporation with the exception of law enforcement in the case of criminal investigations. Kainoa indicated it would be inappropriate for any information to be shared outside the immediate store location. Further, while all agreed that the store might employ some type of analytic technique to improve recommendations or product placement, participants felt that this should involve data stripped of unique identifiers.

3.1 CONFLICTS WITH NOVEL PRACTICES RELATED TO THE INTERNET OF THINGS

3.1.1 LOCATION-BASED SERVICES

A number of changes in the types of data collected, actors involved, and transmission techniques led to concerns by the participants. Location-based services were the component of the Internet of Things that was most salient to participants, since they already had personal experience with these tools and an awareness of related current events, for example recent news stories about Apple and Google using location-based applications on smartphones (e.g., Albanesius, 2011). Although all participants willingly used location-based services in some form on their present mobile device, there was a great deal of concern about who would have access to this data in the future. Proposed services that might announce who is in a store at a given time or seek to provide other social networking services during in-store visits were seen as extremely unwelcome. Concern about targeted communications arose as well, as several participants mentioned that they worried that unknown corporate affiliates might reach out to them based on location-based services linked to personal profiles and that these targeted advertisements might be unwanted or difficult to manage. Marx (2006) argues that location-based information is particularly sensitive because it can both identify an individual and monitor movement over time.

> The substantive information it provides can be compared to predictive models (or used to build them) that then serve to direct how the individual is responded to….

> But it also offers a means of action – knowing where the person is may permit 'reaching' them, either literally, as with 911 responders, or through targeted communications. (pp. 97-98)

In addition to corporate sharing of the data, there was also concern that others could access it through illegal means, leading to fears of stalkers or theft. Keoni worried that unauthorized people might gain access to this information and be able to use it in real-time for burglaries: "they know you're not in your house so they could target you…" Anuhea and Maka mentioned that, even with laws requiring protection of data, there is the potential for theft or hacking.

Maile expressed concern that people might be willing to share location-based data with others initially, but that this could have unintended consequences:

> And I hope it's just not a negative view to take but I do specifically remember that a friend told me that it's the greatest thing even that he could find his friends walking down the street and I thought "don't you think that's crazy? I wouldn't want someone to know that about me. I mean, he hadn't thought about it… and realizing that a lot of people do walk right into that, thinking, "oh, it's not so bad…"

Several participants raised the fear of stalking, particularly by those who might be acquaintances. Perhaps relationships would change over time, or there would be subtleties in the information one would willingly share. On a related note, another theme that emerged was concern about deception in communication. Kainoa emphasized that one's location is personal and he admitted to lying on occasion when people call to ask where he is. Similarly, both Kainoa and Maka described incidents where they saw an acquaintance while shopping and quickly moved to avoid being seen. Deception, including altruistic lying, is a part of everyday communication (DePaulo & Kashy, 1998); and as Dourish and Bell (2011) point out, this will become increasingly difficult in a ubiquitous communication environment.

3.1.2 TRANSPARENCY

Transparency was a key issue, both as it relates to what data is being collected and who has access to it. Kainoa explained that "it's not really clear what they say about their corporate affiliates. That can be anybody. I wouldn't want information going to the government. I wouldn't want it going anywhere, to be honest… My biggest discomfort is knowing that my data is stored somewhere and it's not going to go away. I can't get it off. I might not know where it is." Similarly, Keoni pointed out that it would not necessarily have negative consequences. However, the uncertainty troubled him: "I don't see that that's necessarily a bad thing, but they are gathering it and I just don't know who has it… it's like you just don't know to what use this information is to be put." In Turow's (2006) analysis of customer relationship media, he observed that marketers and advertisers are trying to find ways to "insert themselves unfiltered into their desired customers' domestic lives in ways that encourage consumers to accept surveillance and relationships tailored to their personal characteristics" (p. 295). Direct marketing, product placement, customized media, and loyalty programs are all converging to

enhance marketers’ and advertisers’ surveillance power. At the same time, these “seemingly benign relationships in the new digital environment can quickly lead to feelings of discrimination, anger, and suspicion of institutions” (p. 303). Haggerty and Ericson (2006) note that surveillance enables monitoring pre-constituted social groupings, with the logic of a particular system subjecting individuals to varying levels of scrutiny.

3.1.3 HEALTH-RELATED INFORMATION

Concern about health-related information emerged as a major theme. There was recognition that a great deal of personal information, related to both one’s health and identity (including sexual, religious, or cultural practices) might be inferred from one’s aggregate data. Although going to the supermarket is an “ordinary” and public occurrence, according to Anuhea, electronic monitoring, storing, and analysis of data gathered during routine excursions can be highly personal. She noted,

> I can’t see myself buying anything unusual, but if I do, I don’t want to have that be a judgment later on. I see a trend for women, maybe you’re buying certain feminine products and then you stop buying them, so maybe they know you’re hitting a certain age. I mean, that’s personal information that maybe you don’t want to share.

While store employees or other patrons might witness a consumer making a sensitive purchase, the aggregation and mining of the data allows for historical patterns to be identified and stored.

Kepano also expressed concern about his purchase information being transmitted to other parties. While, in the United States, the *Health Insurance Portability and Accountability Act* of 1996 (HIPPA) prevents specific actors from sharing health information about an individual, other actors not explicitly covered could amass and analyze data:

> … if I’ve got a health issue and I’m buying donuts, you know… my rates may go up, they may drop me. I don’t drink but I may buy a bottle of wine or buy cigarettes… I do that all the time for a friend. I don’t smoke, never have... If that started getting linked to my health organizations, to my insurance… I’ve told my life insurance I don’t smoke or drink. If they start getting the idea that I do smoke and drink, well, my rates are going to go up.

This raises the concern that erroneous personal data could be linked to an individual. Haggerty and Ericson (2006) highlight the likelihood of error in personal profiles of aggregated databases. Solove (2011) also points out that data mining is prone to inaccuracies. Further, it might also enable targeting based on First Amendment-protected activities. Equality is thereby challenged, as information about race, ethnicity, religion, or political views can be inferred. Further, ubiquitous gathering and sharing of data would make transparency difficult, if not impossible, to achieve. One would not be aware of what information is being stored about them, be able to correct factual errors, or delete information deemed invasive. Recent news stories have demonstrated the

commercial value of such information. For example, the Nielsen Corporation, a global advertising and marketing company, was caught harvesting private medical postings from behind a password-protected forum dedicated to discussion of patients' medical conditions (Angwin & Stecklow, 12 October 2010). There is also evidence that data aggregators are developing technology that "matches people's real names to the pseudonyms they use on blogs, Twitter and other social networks" (para. 20). This targeted surveillance would represent a major shift in power, in which corporations would be provided with a view-all of consumer behavior without a corresponding increase in benefits to the consumer. This has the potential to lead to discriminatory behavior on the part of corporations, who might offer different products, or prices, to individuals based on advertiser-generated profiles (Turow, 2006).

3.1.4 BIOMETRIC DATA

In addition to the potential for networked sensors to be placed in or on the body in order to monitor specific medical conditions such as diabetes, participants expressed concern about monitoring shoppers' facial expressions or eye movement. Anxiety about the analysis of facial expressions and affect identification was raised in four interviews. Maka described his concern that cameras linked to facial recognition systems capable of analyzing both identity and microexpressions could be repositioned to examine his behavior based on what products he looked at or touched:

> Reading your microexpressions, your expressions, and understanding how you really feel about this product even thought you might not know it yourself. So that's a little spooky, plus they know your feelings, your personal feelings rather than just what you're purchasing… that's creepy. And just the pervasiveness of all of it… It's like mining your thoughts more than just your buying habits.

In the supermarket context, there have already been technical developments and marketing experiments seeking to accomplish this very thing. Emotion-recognition software has been developed and tested to examine consumers' reactions to advertisements and products on billions of devices (e.g., nViso, 2011). In 2003, a Wal-Mart store in Oklahoma used RFID in cosmetic packages to trigger video cameras in-store to observe and record consumers, an act met with outrage by privacy advocates (Hildner, 2006). Iolana also noted that even if she were somehow able to avoid sharing or use false information about her identity to make purchases, facial recognition technologies could still link all of her behaviors to an actual identity profile. There would be no way to opt-out of sharing this information. Facial recognition technologies are currently under study by the Federal Trade Commission due to consumer privacy concern (Federal Trade Commission, 2011).

3.1.5 AUTONOMY AND IDENTITY

All eight of the participants saw certain aspects of Internet of Things developments as welcome conveniences but also expressed concern that they could lead to invasive targeted marketing. A primary concern was that advertisers with access to stores of personal data, browsing and purchasing trends, and one's location might seek to influence consumer behaviors in an unwelcome manner. Keoni said that, "I don't see

that that’s harmful per se, but it seems somewhat intrusive. Somewhat driven by companies looking for information about you, and once you’ve even thought about their product, that there’s a push for you to purchase it.” Kainoa was more reluctant, noting, “It’s like people are rats on wheels being directed what to do by their phone.” Maka added that “I think for myself I’d like it to know as little as possible about me. I can make my own decisions.” This was echoed by Maile, who observed that,

> I think underneath it all that the concern would be that there is too much information about your identity going out and how is it really linking you to other people and other places because I don’t necessarily want people to know my habits… and I can live without the store telling me that I need to come back.

Essentially, these are concerns about freedom and autonomy. Furthermore, consumers’ constant awareness of, and interaction with, these profiles could limit individual choices. Haggerty and Ericson (2006) note that surveillance can foster the establishment of new forms of identity, with new identity categories being created by advertisers. One’s position in this “new constellation of market segments” determines the commercial offers and communication one receives (p. 16). Increasingly, consumers could be influenced by these messages in ways that limit their own abilities to shape their identities.

3.1.6 PUBLIC SPACES AND THE PUBLIC GOOD

Although the supermarket is considered a public space, it is also a bridge to one’s home life, which is presumably not open to the public gaze. Because the Internet of Things is expected to link a variety of household objects, including refrigerators and other appliances, to global networks, the home itself may become a site of surveillance linked to the supermarket. This would enhance the likelihood of information related to sensitive issues such as medicine, religion, political views, and so forth being captured or exchanged. Through surveillance, the supermarket is transformed from a mundane place, where one has an expectation of privacy to a site of surveillance, highlighting the blurring boundary between public and private space. Anuhea elaborated this idea with an example from the recent Asia-Pacific Economic Cooperation (APEC) conference in Honolulu. She described a news release about a company interested in embedding the pavement in Waikiki with sensors, in order to detect the presence of individuals and move surveillance cameras accordingly.

> It’s putting a new spin on public life. And public space… You think you’re just going around doing your average chores in daily life… Because if I go to a public space there’s an awareness that you’re going to be filmed perhaps, but if I am just going to the grocery store doing my daily chores I have an expectation that it’s more private. So I guess if you’re looking at saying it’s for the public good for events like that, it’s interesting... I don’t know if it makes me feel comfortable but it probably does make the job easier for emergency management teams or the police… but just for going to the grocery store, I am not too comfortable with every move being followed... I just think that because it’s a routine activity that it’s different and that because it’s items that I am purchasing it’s different, because these are items I am using and maybe I don’t want people to know what

> I am using. I’m not saying that Waikiki [site of APEC] is different, but if there’s a large event or a lot of potential crimes that can occur there, maybe it’s a public safety issue, whereas I don’t really think that the grocery store is a public safety issue. I think [security at APEC] was about the public benefit or public good… whereas the grocery is for corporate good.

Anuhea’s claim that neither she nor society at large is benefitting from access to this information again highlights an imbalance in power that emerges from this particular act of surveillance. The question becomes: How much information is actually needed to optimize the shopping experience or to protect the public, and what is actually being collected (for monetary value) that is not of use to the consumer or public safety? Solove (2011) points out that the major policy discourse in the United States right now frames privacy as something one must be willing to give up in order to have security. He emphasizes it is possible to have both, and that we must carefully evaluate security measures to ensure not only that they do not unnecessarily hinder privacy but that they also are effective.

4. CONCLUSIONS

This study examined concerns about privacy and the emerging Internet of Things. Citizens’ reflection on changes in the key actors involved, information attributes, and principles of transmission revealed a number of points where existing norms about the collection and use of personal information will potentially be violated in everyday consumer transactions employing the Internet of Things.

None of the participants in this study objected to the entire vision; in fact, there was some marked enthusiasm. Although participants noted a variety of potential conflicts, all also mentioned specific contexts or applications that were desirable. Nalani describes this “tradeoff”:

> I mean it all seems awkward because it is letting go of so much but it also makes it so much easier. I feel it would just be taking getting used to and as long as I felt I still had control that I would come to accept it… Like you would get more control of your life by knowing all these things, but you’d kind of have to give up control, private information. You’ve got to give a little control to get a little control, I guess.

Others also described these changes in terms of a tradeoff. However, many of the concerns identified above – mining of medical data, invasive target advertising, loss of autonomy through marketing profiles or affect monitoring – appeared to tip the balance between consumer benefit and corporate gain: “Certain things are just not a good tradeoff – what small benefit can come of them could never outweigh the risk” (Anuhea).

The ability to aggregate and mine data from a number of novel sources led to concerns information related to both one’s health and identity could be gathered and used to discriminate economically and politically. This new surveillance power creates an imbalance between the consumer and the corporation that may also impact individual autonomy. In particular, automated systems pushing recommendations or personal affect monitoring could constrain one’s options, thereby threatening autonomy.

4.1 POLICY IMPLICATIONS

Several implications for policy arise from these findings. First, there are clearly some aspects of the Internet of Things in an everyday shopping context that are problematic for some consumers. Thus, some resistance is to be expected. Bennett (2008) notes, for example, the privacy advocacy organization CASPIAN, which focuses explicitly on supermarket consumers and stresses protests and boycotts in the United States. He also explores the possibility of this type of privacy advocacy becoming a global social movement. Recalling Weber and Weber's (2010) questions about laws in the context of the Internet of Things, the time to create legal protections is before major problems arise. Neumann & Weinstein (2006) emphasize the importance of fostering a society-wide discussion about the contexts and conditions within which RFID systems are acceptable.

> This is an especially difficult task, because many of the would-be applications are emotionally charged, and RFID capabilities and ostensible benefits are in some cases being hyped far beyond what is realistic. Yet it is such critical deliberations that will likely influence whether RFID will be deployed primarily in useful tools, or rather as identity shackles. (p. 136)

This is particularly important to consider in light of Maile’s argument that the norm for privacy is still there but that people are just not aware of the many changes that are happening around us, and don’t think through the implications of their engagement with technology. Considering the possibility of resistance, an informed citizenry is critical not only from an ethical perspective, but from a business perspective as well.

The International Telecommunication Union’s (2005) analysis of privacy in ubiquitous network societies emphasizes that three domains must be addressed in tandem when seeking privacy solutions: the sociological, technical, and regulatory. Public education and discourse about what is desired and acceptable is a key part of the sociological solution. From the technological side, the development of privacy enhancing technologies (PETS) and designing new systems with public input is emphasized.

The regulatory domain is likewise complex -- for example, should the United States should consider omnibus privacy protection laws like those employed by the European Union, or would domain-specific laws prove more effective? It is clear that the present standard of industry self-regulation is not sufficient to constrain the threat to privacy. “There is little reason to expect that retailers, if left unbound by the force of law, would be immune to breaches of consumer trust…” (Hildner, 2006, p. 160). However, an omnibus privacy law may be unenforceable or lack the ability to target specific technologies or practices. Since much of the participants’ concern appears to be related to data storage, sharing, and analytics, one possibility is a general law for consumer data sharing coupled with sector-specific laws related to RFID (or other relevant technologies, as they arise). In the case of the consumer shopping experience, the balance is currently on the stores themselves to provide evidence showing that eye tracking or emotion recognition in public places is beneficial to consumers.

5. REFERENCES

Albanesius, C. (2011 May 10). Senator has ‘serious doubts’ about privacy of Google, Apple location apps. *PC Magazine*. Retrieved on June 8, 2011 from http://www.pcmag.com/article2/0,2817,2385150,00.asp

Angwin, J., & Stecklow, S. (2010 October 12). ‘Scrapers’ did deep for data on Web. *The Wall Street Journal*. Retrieved on October 20, 2010 from http://online.wsj.com/article/ SB10001424052748703358504575544381288117888.html

Ashton, K. (22 Jun 2009). That ‘Internet of Things’ thing. *RFID Journal*. Accessed from http://www.rfidjournal.com/article/view/4986 on May 11, 2010.

Barnett, E. (11 Jan 2010). Facebook's Mark Zuckerberg says privacy is no longer a 'social norm'. *The Telegraph*. Retrieved on March 10, 2010 from http://www.telegraph.co.uk/technology/facebook/6966628/Facebooks-Mark-Zuckerberg-says-privacy-is-no-longer-a-social-norm.html

Bennett, C.J. (2008). *The privacy advocates: Resisting the spread of surveillance*. Cambridge, Ma.: The MIT Press.

“China working on unified national Internet of Things strategic plan.” (2010 July 5). TMCnews. Retrieved on August 10, 2010 from http://www.tmcnet.com/usubmit /2010/07/05/4884535.htm

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM, 31*(5), 498-512.

DePaulo B.M., & Kashy D.A. (1998). Everyday lies in close and casual relationships. *Journal of Personality and Social Psychology 74*(1), 63-79.

Dourish, P., & Bell, G. (2011). *Divining a digital future: Mess and mythology in ubiquitous computing*. Cambridge, Ma.: The MIT Press.

European Parliament. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0207+0+DOC+XML+V0

European Commission Information Society and Media. (2008). *Internet of Things in 2020: Roadmap for the future. European Technology Platform on Smart Systems Integration.* Version 1.1 (27 May, 2008).

Federal Trade Commission. (2011 November 21). FTC announces agenda, panelists for facial recognition workshop. Retrieved on November 24, 2011 from http://www.ftc.gov/opa/ 2011/11/facefacts.shtm

Federal Trade Commission. (2010 December 1). FTC staff issues privacy report, offers framework for consumers, businesses, and policymakers. Retrieved on November 24, 2011 from http://www.ftc.gov/opa/2010/12/privacyreport.shtm

Haggerty, K.D., & Ericson, R.V. (2006). The new politics of surveillance and visibility. In K.D. Haggerty and R.V. Ericson (Eds.) *The new politics of surveillance and visibility* (pp. 3-25). Toronto: University of Toronto Press.

Hildner, L. (2006). Defusing the threat of RFID: Protecting consumer privacy through technology-specific legislation at the state level. *Harvard Civil Rights-Civil Liberties Law Review, 41*, 133-176.

Internet of Things Conference Organizing Committee. (2010). Internet of Things. Retrieved on March 17, 2010, from http://www.iot2010.org/outline/

International Telecommunication Union. (2005). Privacy and Ubiquitous Network Societies: Background paper. ITU Workshop on Ubiquitous Network Societies, 6-8 April 2005. Geneva: International Telecommunication Union.

Keller, J. (2011 September 29). Cloud-powered facial recognition is terrifying. *The Atlantic Monthly*. Retrieved on October 1, 2011, from http://www.theatlantic.com/technology/archive/2011/09/cloud-powered-facial-recognition-is-terrifying/245867/

Kling, R. (2000). Learning about information technologies and social change: The contribution of social informatics, *The Information Society, 16*(3), 217-232.

Marx, G.T. (2006). Varieties of personal information as influences on attitudes towards surveillance. In K.D. Haggerty and R.V. Ericson (Eds.) *The new politics of surveillance and visibility* (pp. 79-110). Toronto: University of Toronto Press.

Neumann, P.G., & Weinstein, L. (2006). Risks of RFID. *Communications of the ACM, 49* (5), 136.

nViso. (2011). Technology. Retrieved on October 11, 2011 from http://www.nviso.ch/

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, Ca.: Stanford University Press.

O'Connor, M.C. (2011 April 6). European Commission issues framework for measuring and mitigating RFID's privacy impact. *RFID Journal*. Retrieved on April 6, 2011 from 2011http://www.rfidjournal.com/article/view/8345

Shen, G., & Liu, B. (2011). The visions, technologies, applications and security issues of Internet of Things. *IEEE International Conference on E-business and E-government (ICEE), 2011, 1-4.*

Solove, D. (2008). *Understanding privacy*. Cambridge, Ma: Harvard University Press.

Solove, D. (2011). *Nothing to hide: The false tradeoff between privacy and security*. New Haven, Ct.: Yale University Press.

Turow, J. (2006). Cracking the consumer code: Advertisers, anxiety and surveillance in the digital age. In K.D. Haggerty and R.V. Ericson (Eds.) *The new politics of surveillance and visibility* (pp. 279-307). Toronto: University of Toronto Press.

Weber, R.H., & Weber, R. (2010). *Internet of Things: Legal perspectives*. Berlin: Springer-Verlag Berlin Heidelberg.

Maile	Asian female in her thirties; librarian
Kainoa	Caucasian male in his twenties; full-time student
Nalani	Caucasian female in her twenties; full-time student
Maka	Asian/Caucasian male in his thirties; pilot
Kepano	Caucasian male in his forties; truck driver
Keoni	Native American/Caucasian male in his fifties; mechanic
Anuhea	Caucasian female in her twenties; government IT specialist
Iolana	Asian/Caucasian female in her forties; editor

Table 1. Participants